Math 116: Worksheet 7

Owen Jones

March 14, 2024

1. Compute $E_K(X_i)$
   $O_i = L_k(E_K(X_i))$
   $P_i = O_i \oplus C_i$
   $X_{i+1} = R_{b-k}(X_i) \parallel C_i$
   We also need to know X_1 and K

2. Compute $E_K(X_i)$
   $O_i = L_k(E_K(X_i))$
   $P_i = O_i \oplus C_i$
   $X_{i+1} = R_{b-k}(X_i) \parallel O_i$
   We also need to know X_1 and K

3. We don't use a decryption function. The encyption function doesn't need to be invertible.

4. (a) OFB

   (b)